CCTV Compliance Policy

1. Introduction

This policy governs the operation of the closed circuit television (CCTV) systems operated by Chipping Norton Town Council as data controllers to assist in carrying out enforcement, public safety and other functions.

The policy sets out the principles to be observed by each Council, its members, employees, contractors, and any other parties or organisations involved in the operation, management and administration of relevant CCTV systems. It is also intended to inform members of the public of the purposes for which CCTV is operated, and of the standards which will be met in relation to it. In this way, each Council can be held accountable for its compliance with the policy.

A list of key definitions and acronyms is set out at section 13 of this policy.

2. Purpose

Compliance with this policy and with the detailed arrangements which sit under it ensures that each Council's use of Closed Circuit Television Cameras reflects a proportionate response to identified problems, which is operated with due regard to the privacy rights of individuals.

3. Background

In recent years there has been a substantial increase in the number of CCTV cameras, driven in part by a reduction in the costs of installing and operating this type of equipment. This increase has coincided with heightened privacy concerns, which have resulted in laws, regulations and codes of practice designed to ensure that the use of cameras is legitimate, proportionate to the intended purpose and respectful of legitimate privacy expectations. Article 8 of the Human Rights Convention recognises the right to a private and family life. Where CCTV captures images of people which comprise personal data, there is potential for this to infringe on the privacy of individuals. Accordingly, there is an obligation for CCTV installations and handling practices to comply with the 3rd Data Protection Principle (data minimisation) as well as the 6th Principle (Appropriate technical and organisational security) as set out in the Data Protection Act and General Data Protection Regulations.

CCTV systems are operated by the Council only as a proportionate response to identified problems, this in so far as it is considered necessary in a democratic society in the interests of public safety, for the prevention and detection of crime and disorder and for the protection of

the rights and freedoms of others. The Information Commissioner's Office ('the ICO') has enforcement powers which include the power to issue directives to remove or modify CCTV installations. The ICO is supported by the Surveillance Camera Commissioner, which was established under the Protection of Freedoms Act 2012 and has issued codes of practice for the use of these cameras, which include the guiding principles set out below.

4. CCTV

Within the scope of this policy the Council acts as data controller for the CCTV systems it operates for the purposes of preventing and detecting crime and for ensuring public safety, including that of attendees at its public venues.. For the avoidance of doubt it does not include CCTV for which third parties are the data controllers e.g. the Police.

5. General Principles/ Guidelines

The Council's use of CCTV accords with the requirements and the principles of the Human Rights Act 1998, the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and the Protection of Freedoms Act 2012. This policy recognises the need for formal authorisation of any covert 'directed' surveillance as required by the Regulation of Investigatory Powers Act 2000, and provides that CCTV shall be operated fairly, within the law and only for the purposes for which it was established or which are subsequently agreed in accordance with the Code.

CCTV shall be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home. Public interest in the operation of CCTV will be recognised by ensuring the security and integrity of operational procedures which sit underneath it, and which balance the objectives of the CCTV usage with the need to safeguard the individual's rights.

Transparent: This policy ensures that CCTV used by or on behalf of the Council is transparent. Wherever possible, the presence of CCTV, the purpose for it and contact details for the Controller of it should be clearly displayed to the public. There are strict laws around the use of covert surveillance cameras and these should only be implemented where necessary for a criminal enforcement purpose where the Council has the necessary statutory authority and under the oversight of the Senior Information Risk Owner (SIRO).

For a Legitimate and Specified Purpose: prior to establishing any CCTV installation, it is necessary to establish a legitimate purpose for it. The appropriate balance between the necessity of the CCTV and the privacy rights of individuals can only be assessed in light of this intended purpose. the usage of CCTV cameras, including the field of vision and whether they can be controlled remotely, has to be proportionate to the identified need. For example, installation of a camera for the purpose of public safety would be unlikely to be proportionate in an area with no particular history of incidents. CCTV will not be installed unless found to be proportionate following a Data Privacy Impact Assessment.

6. Surveillance Camera Code of Practice

Each Council will operate all CCTV implementations in line with the principles set out in the Surveillance Camera Commissioner Code of Conduct:

- Use of a CCTV system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a CCTV system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a CCTV system as possible, including a published contact point for access to information and complaints. There must be clear

responsibility and accountability for all CCTV system activities including images and information collected, held and used.

- Wherever a CCTV system is used, these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a CCTV system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted.
- The disclosure of images and information should only take place when it is necessary and proportionate for such a purpose or for law enforcement purposes. CCTV system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- CCTV system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a CCTV system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a CCTV system which compares against a reference database for matching purposes should be accurate and kept up to date.

7. Privacy Risk Assessed

All existing and proposed CCTV installations should be subject to a Data Privacy Risk Assessment to identify what risks to privacy they pose and what controls can be applied to minimise them. Copies of the Assessment should be held by the Council Senior Information Risk Owner (SIRO).

All proposals to install new or additional CCTV must be approved by the Town Clerk and CEO. Where the privacy assessment indicates a high risk to privacy, then the approval of the SIRO is required prior to the procurement of CCTV equipment.

As CCTV recordings contain personal (and sometimes special category) data, there is a legal obligation to ensure that access is limited to those with a genuine need and that any data held meets technical standards for information security. In the event of a data breach, then prompt steps will be taken in accordance with each Council's procedures to mitigate the breach and to notify relevant parties.

Subject to clear operational procedures which are binding on staff and contractors: all Council departments operating CCTV are required to ensure that there are procedures in place which regulate where cameras can be installed, where they should point, under what circumstances data can be accessed or removed from the devices and under what circumstances it can be disclosed to other parties.

Auditable: All staff actions which affect the operation of CCTV equipment should be captured in audit logs held on the devices or in controlling applications. This includes any actions which change the field of vision, any downloads of footage and any deletion of footage. All CCTV equipment must

be specified so as to provide accurate time and date stamping, and all CCTV installations will be recorded on the CCTV Register.

CCTV systems operated by the Council shall normally retain footage for no longer than 30 days. Where footage is required for the purposes of prosecution of an offence or to defend legal claims, a copy should be made and stored securely.

8. Cameras and Area Coverage

Care should be taken to ensure that cameras are sited so they are clearly visible. No hidden cameras will be used, nor shall cameras be directed in such a way as to amount to surveillance which is intrusive.

Clear signage will normally placed within the area which is being monitored in order to ensure that both the public are aware when they are in a monitored area and also that the maximum deterrent value is achieved. Where this is not possible – as in the case of body worn cameras, and signage on vehicles – then the cameras themselves will be clearly signed. The Council's CCTV systems do not record audio.

Camera positions will be reviewed annually to ensure that they remain proportionate to their purpose. Where the purpose can no longer be justified against the intrusion on personal privacy, they will be removed or switched off. All viewing and recording equipment shall only be operated by trained and authorised users.

9. Roles and Responsibilities

All staff members with operational access to CCTV equipment are responsible for following the specific operational procedures established for its use. This includes checking the equipment and reporting to management where it is found to deviate from the agreed specification or appears to have been interfered with. Staff and other relevant persons shall only be permitted access to images obtained via CCTV on a 'need to know' basis. Information Asset Owners are accountable for identifying a legitimate need for CCTV installations where one exists (and for reviewing the same), for ensuring that data privacy impact assessments are conducted and an action plan generated and progressed and for making sure that risk controls are established where needed to protect personal privacy.

The SIRO is responsible for setting the risk appetite for CCTV installations for the Council and assessing high risk proposals. The Data Protection Officer (DPO) is responsible for assessing proposed CCTV installations posing a high risk to privacy, rights and freedoms and for making recommendations to the SIRO.

In cases of a serious breach involving CCTV data, the DPO is responsible for reporting the matter to the ICO. The Town Clerk and CEO is responsible for maintaining the CCTV Register, drawing up Data Privacy Impact Assessments and participating in the investigation of breaches.

10. Training Requirements

All individuals with a need for operational access to CCTV systems or for access to images captured via CCTV shall be trained to a proficient level which meets appropriate safeguards before they are permitted access. All relevant individuals are furthermore required to have read the Surveillance Camera Code of Conduct and to have had sufficient training in the specific equipment they operate.

11. Data Protection and subject access rights

The public have the following rights with regard to CCTV footage captured by the Council's cameras:

- A right to request through subject access, a copy of footage in which they are captured, subject to exemptions within the Data Protection Act 2018 and also balanced against the rights and freedoms of others who may appear in that footage. All requests for CCTV images should be made in writing to the Town Clerk and CEO.

- A right to object to processing where they believe that the field of vision or the siting of the camera is disproportionate to the stated purpose of the camera. Where a resident objects to processing, the Council will consider the objection and decide whether a lawful basis for processing can still be justified. A written response will be provided outlining the outcome.

12. Data Retention & sharing

The police, social services, environmental health and/or other authorised agencies or bodies may apply for access to data collected via CCTV in order to carry out their statutory functions. All requests will be reviewed by the Council's Data Protection Officer and determined according to a process which ensures compliance with the law.

All Council CCTV Cameras automatically over-write footage after 30 days after it is captured. Where authorised bodies are granted access to data collected via CCTV in order to carry out their statutory functions, then copies of the data may be made and provided securely for this purpose.

Any data downloaded for the purpose of criminal investigation, subject access request or Council investigation will be retained for 3 months.

13. Key Definitions

CCTV – Closed Circuit Television

Data Protection Officer (DPO) – A statutory role set out under the Data Protection Act with responsibility for ensuring that organisations are compliant with personal privacy rights. Any resident can report a personal privacy concern about the Council to the Data Protection Officer.

General Data Protection Regulation (GDPR) - A Regulation establishing data protection principles and privacy rights for people whose data is processed in the European Union. It is supplemented in British law by the Data Protection Act 2018 which enshrines its rights and principles.

Information Asset Owner – A role held by the Business Managers, to ensure that information systems operated by their teams have appropriate data quality, auditability and access controls.

Senior Information Risk Owner (SIRO) – A role established under International Information Security Standard ISO27001 to ensure that appropriate processes for information risk and the treatment of that risk are established and maintained. At the Council, the role is held by the Business Manager - Corporate Responsibility

14. Review of this Policy

This policy will be reviewed annually.

15. Related Policies

Data Protection Policy